شرح طريقة تطويع برنامج تور

في هذا الشرح سوف نبين طريقة تطويع برنامج تور وجعله فعال جدا وتفادي الوقوع في بيريدج مخابراتي وهذا ما سنفعله هنا علاوة على ذلك سنؤمِن الخروج من شبكة التور ونتفادى نقاط التفتيش في وسطها حتى نساهم في تأمين المسار و رفع السرعة وبالتالي سرعة التصفح.

محتوى الموضوع

1. البريدجات بين الحماية وخطر التجسس.
2. سبل الوقاية:
   - A طريقة للبحث عن بريدجات
   - B حذف البريدجات المشبوهة و وضع السليمة "يدويا" في التور
   - C ازالة مخارج التور التي تكون في بلدان شديدة العداء.
   - D مخارج التور حيث المعلومة تكون مكشوفة"
   - E ازالة العقد المشبوهة من وسط الشبكة لتأمين المسلك وتسريع التصفح
3. الخلاصة.



1 البريدجات بين الحماية وخطر التجسس

ماهي البريدجات وماهو دورها ؟؟

في بعض البلدان يتم غلق نقاط دخول التور التي تسمى التحويلة **(relay)** ويمكن غلقها لا نها نقاط ثابتة معروفة **(الآيبي الخاص بها معروف)** او يتم مراقبة من يرتبط بتلك التحويلات.

لذلك فإن برنامج التور يقترح سبل أخرى لدخول شبكته وهي **البريدجات** وهي عبارة عن قناطر تعبر بها الى شبكة التور من دون معرفة الجهات الامنية **(هم في الحقيقة اشخاص متطوعون يجعلون من حواسيبهم معبر نحو شبكة التور).**

وقفة لابد منها مع كيفية ارسال المعلومات عبر شبكة التور وتشفيرها

في جهازك يوجد بروكسي اسمه Polipo يقوم بأخذ المعلومات من المتصفح "الفايرفوكس" ثم يرسلها الى اول نقطة في شبكة التور مشفرة وعن طريق بروتوكول حماية اسمه socks.

في شبكة التور تمر المعلومة بعدة عقد وبمسارات متغيره سنفترض هنا ان المعلومة ستمر خلال شبكة التور بثلاث عقد.

تُشفر المعلومات في جهازك بمفتاحك الخاص والمفتاح العام لآخر عقدة في شبكة التور ثم تشفر مرة ثانية بالمفتاح العامة لثاني عقدة في الشبكة ثم للمرة الثالثة بالمفتاح العام لأول عقدة في الشبكة اي ستشفر ثلاث مرات (فنحصل على بصلة بها ثلاث قشور!).

ثم يقوم جهازك بأرسل المشفرة الى اول عقدة في الشبكة (بريدج في حال استعملنا خاصية البريدجات) تقوم تلك العقدة بفتح التشفير مستعملة مفتاحها الخاص لتعرف الى من سترسل المعلومة (فقد تكفل جهازك بوضع عنوان كل عقدة في طبقة خلال عملية التشفير).

تتلقى العقدة الثانية المعلومة من العقدة الاولى, تفك طبقة واحدة من التشفير باستعمال مفتاحها الخاص (تزيل قشرة من البصلة) لتعرف الى من سترسل المعلومة.

تتلقى العقدة الثالثة (عقدة الخروج من الشبكة) المعلومة من العقدة الثانية وقد بقي فيها تشفير واحد (البصلة بقية عليها قشرة واحدة!) تقوم بفك ذلك التشفير باستعمال مفتاحها الخاص لتحصل على لب المعلومة (لب البصلة!) وفي نفس الوقت عنوان الموقع المراد زيارته طبعا لب المعلومة لا يحتوي على الايبي خاصتك الا اذا كنت تستعمل الفلاش او لم توقف الكوكز الخطيره.

يجب عليك ان تقوم بوقف الكوكيز الخطيرة في المتصفح لذا ننبه لذلك يجب إضافة بعض برامج التأمين الهامة جدا وهى اضافات لمتصفح الفايرفوكس مثل: **FlashBlock** و **Nosciript**.

لتحميل الاضافات الخاصة بالفايرفوكس للحماية

FlashBlock	https://addons.mozilla.org/ar/firefox/addon/flashblock
Nosciript	https://addons.mozilla.org/en-US/firefox/addon/noscript

في حالة عدم عمل رابط الاضافة في الموضوع تم ارفاق ملف تكست يحتوى على رابط تحميل الاضافات – اسم الملف **ADD-ONS**

في حالة كان الموقع الوجهة يدعم خاصية التشفير https فإن التور سيرسل المعلومات مشفرة لذلك الموقع.



بروتوكول نقل النص التشعبي الآمن

بروتوكول نقل النص التشعبي الآمن **(HTTPS)** هو مزيج من بروتوكول نقل النص التشعبي مع خدمة تصميم المواقع تلس / بروتوكول لتوفير الاتصالات المشفرة وتحديد تأمين شبكة خادم الويب. غالبا ما تستخدم الشبكي وصلات لمعاملات الدفع على الشبكة العالمية للمعاملات ونظم المعلومات الحساسة في الشركات. الشبكي لا ينبغي الخلط بينه وبين النص المتشعب الآمنة

بداية الفكرة

الفكرة الرئيسية من الشبكي هو إنشاء قناة آمنة عبر شبكة آمنة. وهذا يضمن حماية معقولة من التنصت والهجمات والقراصنة، شريطة أن يتم استخدام الأجنحة الكافية والشفرات والتحقق من هذه الشهادة هو الخادم وموثوق به.
المتأصلة في الشبكي يعتمد على الثقة الكبرى الشهادات الأمنة التي تأتي مثبتة مسبقا في برنامج التصفح (وهذا يعادل قائلا "أنا على ثقة السلطة شهادة (مثل فيريساين / مايكروسوفت / الخ.) ليقول لي أن أعطيه الثقة"). وعلى موقع على شبكة الإنترنت يمكن الوثوق بها لذلك الاتصال الشبكي إذا وفقط إذا كانت كافة الإجراءات التالية صحيحا : وتأمل المستخدم التي تنفذ البرامج الخاصة بهم بشكل صحيح متصفح الشبكي مع السلطات الشهادة المثبتة مسبقا بشكل صحيح.

المستخدم يثق في السلطة ليشهدوا شهادة فقط للمواقع المشروعة دون أسماء مضللة. ويوفر الموقع شهادة صالحة، وهذا يعني تم التوقيع عليها من قبل سلطة موثوق به.
(شهادة غير صالحة يظهر تحذير في معظم برامج التصفح) الشهادة بشكل صحيح يعرف الموقع (على سبيل المثال زيارة الموقع : https://example على سبيل المثال وتلقي شهادة من أجل "مثال شركة" وليس أي شيء آخر اما التدخل القفزات على الإنترنت هي جديرة بالثقة، أو

المستخدم يثق البروتوكول التشفير طبقة (تلس أو خدمة تصميم المواقع) هي غير قابلة للكسر من قبل المتصنت



تضمينه مع المتصفح

عند الاتصال إلى موقع مع شهادة غير صالحة، فإن المتصفحات القديمة الحالية تعرض على المستخدم نافذه "هل يريد الاستمرار أم لا" المتصفحات الحديثة تعرض تحذير عبر نافذة بأكملها. تعرض المتصفحات الحديثة أيضا أحدث المعلومات والتحذيرات في موقع بارز للأمن في شريط العنوان الموقع.

التاريخ

أنشأت شركة نتسكيب للاتصالات بروتوكول نقل النص التشعبي الآمن في العام 1994 للعمل مع متصفحها للمواقع نتسكيب. كان البروتكول في الأصل يستخدم في التشفير عن طريق ال **SSL** وهو اي ال**SSL** تطور ليكون **TLS**.

توضيح لكيفية التعامل مع الرابط الرقمي المشفر

والشرح هام جدا لان المخابرات المعادية والجهات الامنية التي تراقب الانترانت استغلت خاصية التشفير في المواقع والمنتديات المحظورة والمحجوبة في بلدك واصبح يظهر لنا الموافقة على السماح للموقع الذى نود تصفحه عند طلبنا له وهو في الحقيقة محاولات للتجسس



لذلك هنا شرح كيفية التعامل مع الرابط الرقمي المشفر

استعمال الرابط المشفر يعني ان المعلومات المتبادلة مع الموقع المطلوب تكون مشفرة وبالتالي الجهاز الذي تغادرون منه شبكة التور سترسلها مشفرة للموقع ولن يطلع عليها.

في رسم إجمالي يمكن تصوير مسار المعلومات هكذا:

في حال استعملنا الرابط المشفر:

جهازكم <=== بريدج==<==عقدة وسط التور==<==عقدة خروج===<المنتدى

في حال لم نستعمله:

جهازكم <=== بريدج ==<==عقدة وسط التور==<==عقدة خروج===<المنتدى

اللون الاحمر يعني ان المعلومات غير مشفرة.

والتشفير يعني ايضا اجمالا تبادل شهادة يكون واجبا على الموقع الذى تزوره في كل مرة اظهارها والا فانه ليس هو الموقع الموثوق الهدف اذن اجمالا من تلك الشهادة هو معرفة ان الموقع الذي سندخله هو نفسه الذي وثقنا فيه وعنده نسخة من الشهادة وليس موقع مغاير .

تنبيه هام

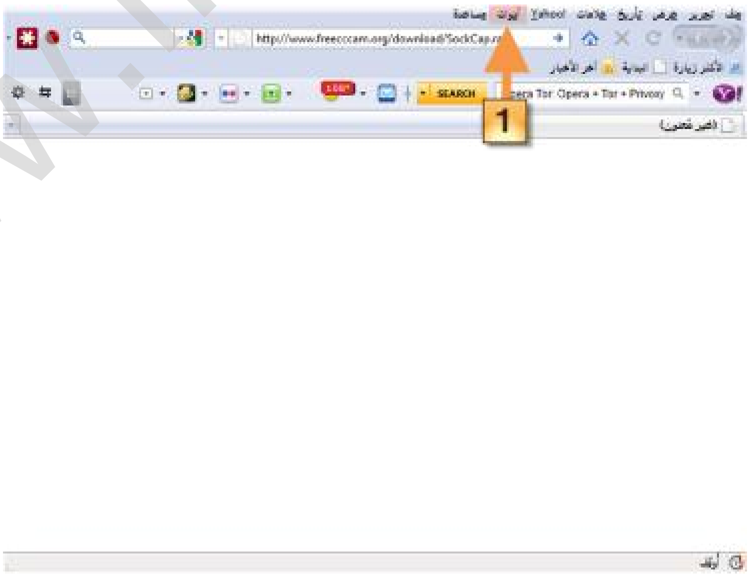
عندما تدخلون الى أي موقع مشفر سوف يطُلب منكم التصديق على الشهادة بعد الاطلاع علبها وحتى لايدس احدهم شهادة مزورة في وسط الطريق يكون الهدف منها التجسس على المعلومات, فهنالك حل بسط يغنيكم عن فحص مفتاح الشهادة في كل مرة والحل يمثل في الطلب من المتصفح تسجيل الشهادة عنده وفى حالة أقترح عليكم أحدهم في مرة من المرات شهادة اخرى فهذا يعني عموما انها محاولة ل تسلل .

وبما انني طلبت من المتصفح تسجيل الشهادة عنده فاني في كل مرة ت عُرض علي شهادة اقوم برفضها و أقوم بتغيير الهواية أو بإغلاق التور وفتحه من جديد فيختفي ذلك الطلب المريب.

شرح كيفية الطلب من المتصفح تسجيل شهادة موقع معين عنده

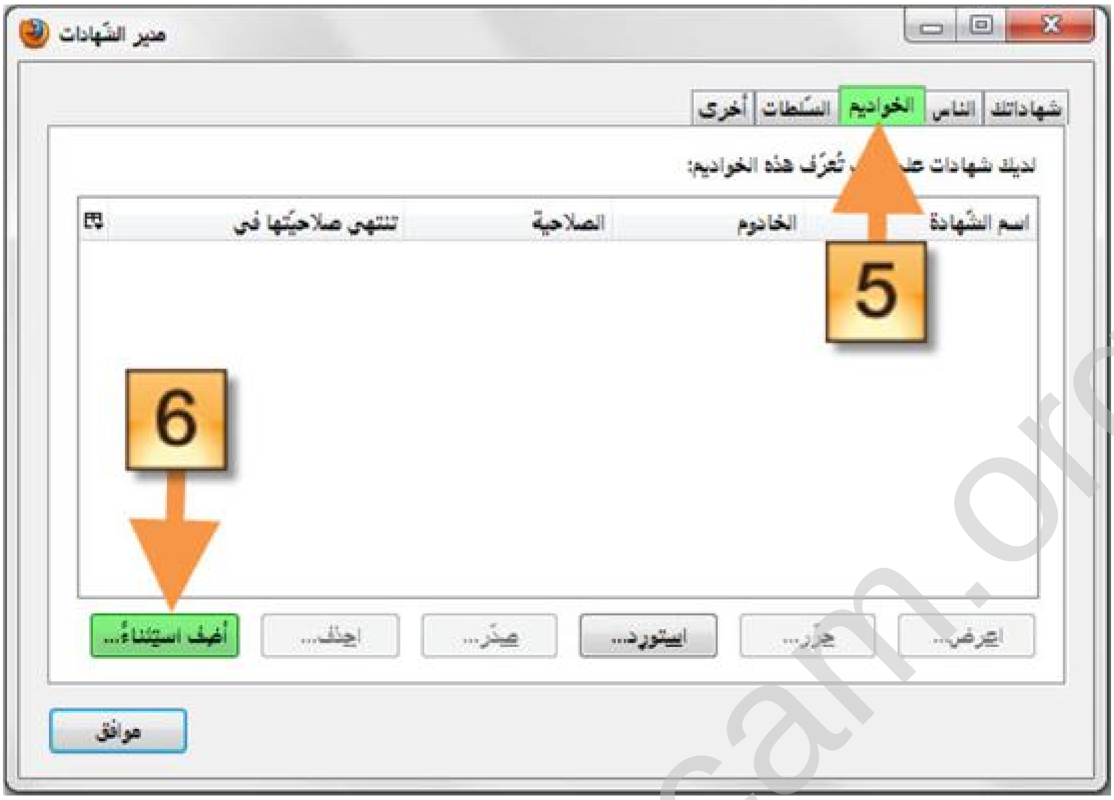
الان سنجعل من المتصفح يقبل شهادة الأمان من موقع معين فقط وبذلك لن تخرج لكم تلك الصفحة في كل مرة تدخلون المنتدى.

تذهبون الى الشريط في المتصفح ونختار أدوات تابع الشرح المصور




موزيلا فيرفكس
ملف
تحرير
عرض
تأريخ
علامات
أدوات
مساعدة
ابحث في الشبكة
Ctrl+K
التنزيلات
Ctrl+J
الإضافات
مرقاب الأخطاء
Ctrl+Shift+J
معلومات الصفحة
ابدأ التصفح الخاص
Ctrl+Shift+P
امسح التأريخ الحالي...
Ctrl+Shift+Del
الخيارات...
2
الأكثر زيارة
البداية
آخر الأخبار
(غير معنون)


الخيارات
عام
الألسنة
المحتوى
التطبيقات
الخصوصية
الأمان
متقدم
عام
الشبكة
التحديثات
التعمية
البروتوكولات
استعمل SSL 3.0
استعمل TLS 1.0
الشهادات
ابسألني كلّ مرّة
حدد واحدة آليًا
أظهر الشهادات
قوائم النقض
التحقق
أجهزة الأمن
2
3
4
موافق
ألغ
مساعدة

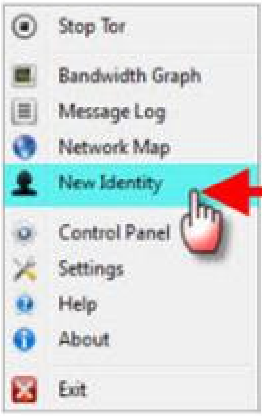

مدير الشّهادات
شهاداتك
الناس
الخواديم
السّلطات
أخرى
اسم الشّهادة
الخادوم
الصلاحية
تنتهي صلاحيّتها في
5
6
اعرض...
احفظ...
استورد...
صدّر...
احذف...
أضف استثناءً...
موافق


أضف استثناءً أمنيا
أنت على وشك تخطي كيفية تعرّف فَيَرفُكس على هذا الموقع.
البنوك الحقيقية، المحلات والمواقع العامة الأخرى لن تطلب منك القيام بهذا.
الخادوم
المكان:
https://www.torproject.org
اجلب الشهادة
حالة الشهادة
اعرض...
احفظ هذا الاستثناء دائما
أكِّد الاستثناء الأمني
ألغِ


أضف استثناءً أمنيا
أنت على وشك تخطي كيفية تعرّف فَيَرفُكس على هذا الموقع.
البنوك الحقيقية، المحلات والمواقع العامة الأخرى لن تطلب منك القيام بهذا.
الخادوم
المكان:
https://www.torproject.org
اجلب الشهادة
حالة الشهادة
اعرض...
شهادة صالحة
يعطي هذا الموقع شهادة صالحة، وهوية موثّقة. لا حاجة لإضافة استثناء.
9
احفظ هذا الاستثناء دائما
أكِد الاستثناء الأمني
ألغِ


"*.torproject.org":عارض الشهادات
عام
تفاصيل
تم التحقق من هذه الشهادة للاستخدامات التالية:
شهادة خادوم SSL
مُصْدَرة إلى
الاسم الشائع (اش) *.torproject.org
المنظمة (م) The Tor Project, Inc.
الوحدة التنظيمية (وت) <ليس جزءًا من الشهادة>
الرقم التسلسلي 00:85:5D:DF:AB:49:60:10:A7
مُصْدَرة من
الاسم الشائع (اش) BitDefender Personal CA.Net-Defender
المنظمة (م) BitDefender
الوحدة التنظيمية (وت) IDS
الصلاحية
مُصْدَرة في 2/15/2011
تنتهي صلاحيتها في 4/20/2013
البصمات
بصمة SHA1 A2:F0:D5:57:CF:84:9E:00:5E:34:D0:B1:C4:D7:D6:10:AA:3B:0B:CF
بصمة MD5 EE:7A:13:A6:2D:80:7D:98:32:10:45:F4:04:80:64:AF
أغلق

تعقيبات هامة



تقوم العقد بتغير مفاتيحها دوريا كل اسبوع وارسالها مشفرة لك حتى تتمكن من تشفير المعلومات

المسلك المتبع للمعلومة يتم تغييره كل عشرة دقائق حتى يتم تغيير العقد المستعملة ويمكن ايضا للمستخدم تغيير المسلك عن طريق خيار new identity

تقوم العقد بتغيير مفاتيحها العامة (onion key) دوريا (كل اسبوع تقريبا) وارسالها مشفرة لك حتى تتمكن من تشفير المعلومة بها.

- البريدج (العقدة الأولى) تعرف الايبى خاصتك لكنه لا يعلم شيء عن محتوى المعلومة لأنها مشفرة بعدة طبقات لا يمتلك مفاتيحها العامة.

- كل عقدة تعرف فقط من اين ترسل المعلومة والى اين (العقدة السابقة) و (العقدة الموالية) ولا تعلم شيء على محتواها ولا عن مصدرها الاول ولا على الوجهة النهائية. العقدة النهائية تعلم محتوى المعلومة ووجهتها النهائية لكنها لا تعلم مصدرها الاول رغم انها تمتلك المعلومة غير مشفرة!

- انت عندما تطالب ببريدجات وتقوم بالضغط على زر البحث عن بريدجات فأنه سيعطيك بريدجات اعتماد على معرفته لهوية جهازك الأيبى الخاص بك لكن هذه الخاصية لها مخاطر عديدة ومنها انه قد تأقلمت الجهات الامنية مع هذه الخاصية واستغلتها فقامت بتنصيب بريدجات تجسس خاصة تقوم بعرضها للاستعمال ومن خلالها يمكن للجهات الامنية المختصة معرفة من يتصل بالتور وربما كشف المعلومات فنحن لا نعلم مدى تعاون التور مع الاجهزة الامنية في هذا ..



◉ البريدج يتلقى المعلومة كاملة ومشفرة من جهازنا ويعرف الايبي خاصتنا.

تحتوي هذه المعلومة على العقد التي ستمر بها خلال الشبكة و الوجهة النهائية لكنها معلومات مشفرة كما قلنا سابقا بمفاتيح مختلفة.

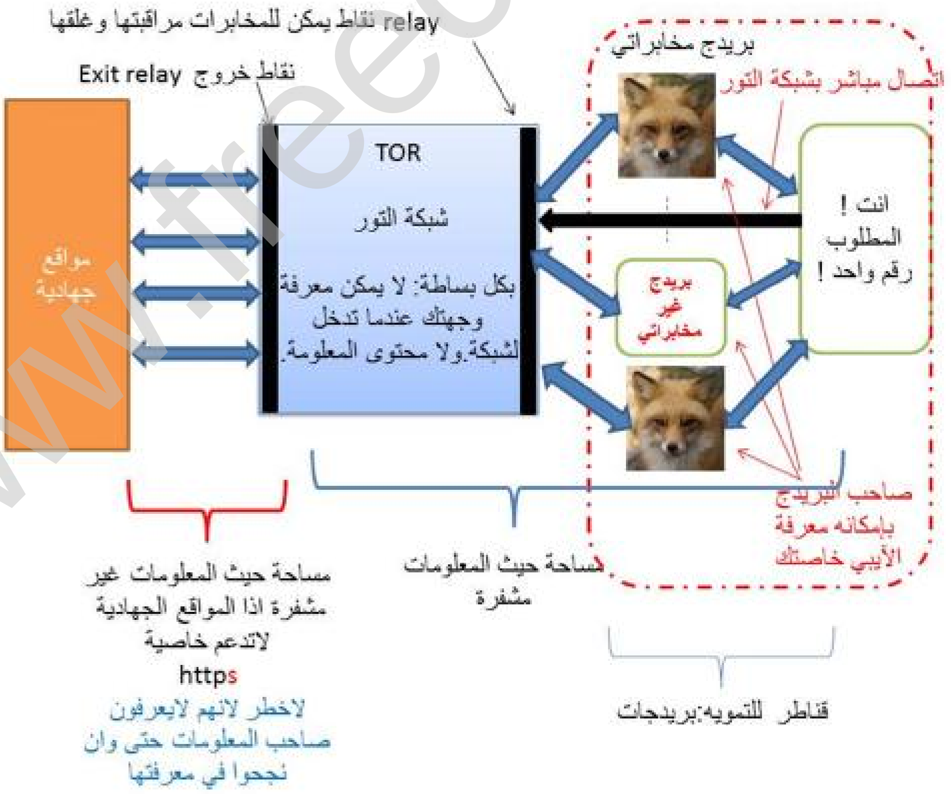
◉ سيصبح هنالك خطر اذا كان البريدج الذي وقعنا فيه تابع للأجهزة الامنية ويتعاون مع مؤسسي التور فإنه بذلك سيتم مدهم بمفاتيح العقد (خاصة وعامة) التي ستمر بها المعلومة وسيتم فك التشفير والحصول على المحتوى ومن ضمن المحتوى الوجهة النهائية طبعا البريدج يعلم الايبي خاصتنا لانه تسلم المعلومة من عندنا.

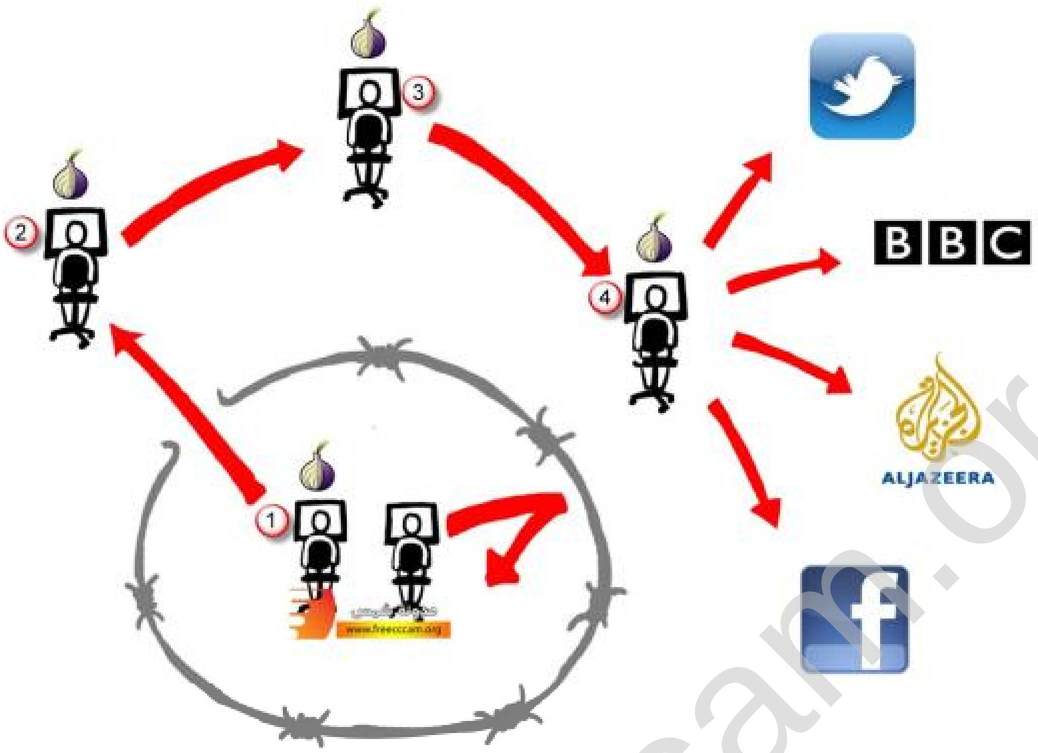
◉ اما بخصوص ال **ISP** مزود الخدمات في بلدك فهو بصفته العادية لن يستطيع معرفة محتوى المعلومة لكنه بإمكانه مراقبة محاولات الاتصال ببوابات شبكة التور.

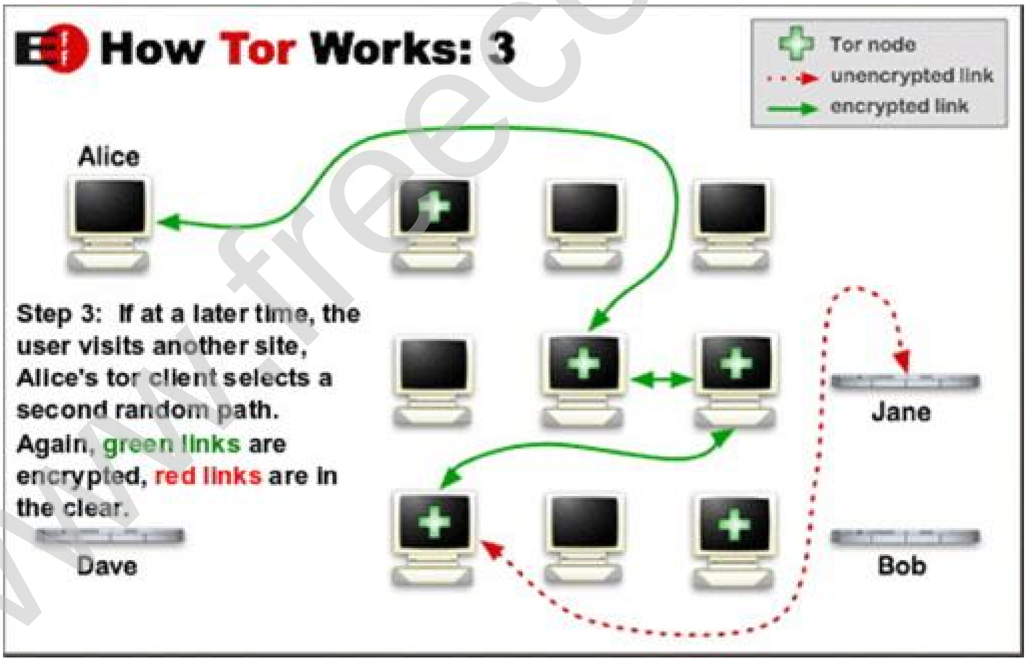
من واجبنا الان محاولة تفادي الوقوع في بيريدج امنى وهذا ما سنفعله هنا علاوة على ذلك سنؤمِّن الخروج من شبكة التور ونتفادى نقاط التفتيش حتى نساهم في رفع السرعة !

◎ التور يقوم اعتمادا على معرفته للآيبي الخاص بك بإعطائك بريدجات شبه ثابته لفترة طويلة وهذا خطر لآنها ستصبح مثل نقاط دخول التور **relay** التي يمكن مراقبها من طرف الجهات الامنية والأخطر من كل ذلك ان التور بإمكانه صرفك إلى بريدجات مخصصة للمراقبة في حالة جاءته الأوامر بذلك (عند الاشتباه في الايبي لخاصتك واعتزام مراقبتها).

هذه الصورة تبين شرح مبسط لعلاقة البريدجات بشبكة التور:







بعض الأدلة على ما قلت

الدليل على ان التور يعطي بريدجات شبه ثابته:

قمت لفترات متفرقة ولمدة طويلة بمراقبة البريدجات التي يعطيها التور عندما نضغط على زر البحث عن بريدجات جديدة فوجدت انه يحافظ تقريبا على نفس البريدجات.

التوقيت عدد1

ip_a

ip_b

ip_c

التوقيت عدد2

ip_d

ip_b

ip_c

التوقيت عدد3

ip_a

ip_b

ip_c

التوقيت عدد4

ip_e

ip_b

ip_c

نلاحظ انه حافظ على نفس البريدجات **ip_b** و **ip_c**. لا يعني هذا حتما ان هنالك مراقبة لكنه أمر غير مُطمئن.

الدليل على توزيعه للبريدجات حسب الآيبي

قمت بفحص البريدجات المتحصل عليها خلال استعمالي لخمسة آيبيهات مختلفة (استعملت "نفق" **vpn** خاص لتغيير الآيبي في كل مرة) النتيجة أن التور خصص لكل آيبي بريدجات معينة لمدة طويلة من هنا بإمكاننا استنتاج امر مهم جدا سنتحدث عنه بالتفصيل من بعد وهو يتمثل في الحصول على بريدجات بمخادعة التور نفسه ! اي تبحثوا عن بريدجات جديدة وانتم مرتبطون بالشبكة وفي كل مرة تغيرون الهوية ! new identity.

الدليل "التقني" على وجود بريدجات تجسس:

عثرت على هذا البريدج وخلال تتبعي لهويته اتضح انه تابع للشبكة **cia** اسمها **ci host**

البريدج:

IP Address : 64.182.160.187Status : SucceedCountry : USA - TexasNetwork Name : CIHSOwner Name : C I HostAddress : 1851 Central Drive, #110, BedfordEmail : noc@cihost.comAbuse Email

2 سبل الوقاية

في هذه الطريقة سنضيف البريدجات يدويا الى ملف اسمه torcc وهي طريقة تمكننا ايضا من برمجة التور كما نشاء وليس كما يشاء.

ملاحظة مهمة : عند تطبيق هذه الطريقة لا تلمسوا ابدا **settings** في واجهة التور.

نختار من الموقع بريدجات غير تابعة للدول المعادية مثل الولايات المتحدة الامريكية واسرائيل والمانيا وإنجلترا وأي دول اخرى ويوجد الكثير من البريديجات الخطرة لذا يجب علينا ان نقوم بعمل تصفية لها لضمان السلامة

الطريقة

موقع البحث عن بريدجات يكون باعتماد صفحة

Web	https://bridges.torproject.org

في حالة عدم عمل رابط الموقع في الموضوع تم ارفاق ملف تكست يحتوى على رابط موقع البريدجات – اسم الملف **BRIDGES**

موقع **تتم تنقية البريدجات (ازالة بريدجات امريكا, المانيا, الصهاينة ومن لف لفهم من اشد اعداءنا) باستعمال برنامج IPNETINFO.**

Web	http://www.freecccam.org/download/ipnetinfo.zip

في حالة عدم عمل رابط البرنامج في الموضوع تم ارفاق ملف تكست يحتوى على رابط تحميل البرنامج – اسم الملف **IPNETINFO**

وانتم شابكين في التور ادخلوا الى موقع البريدجات ثم تابع الشرح المصور 📷 نتوجه الى الموقع الخاص بالبريدجات وننسخ البريدجات الجديدة ولصقها فى البرنامج من اجل معرفة مصدرها

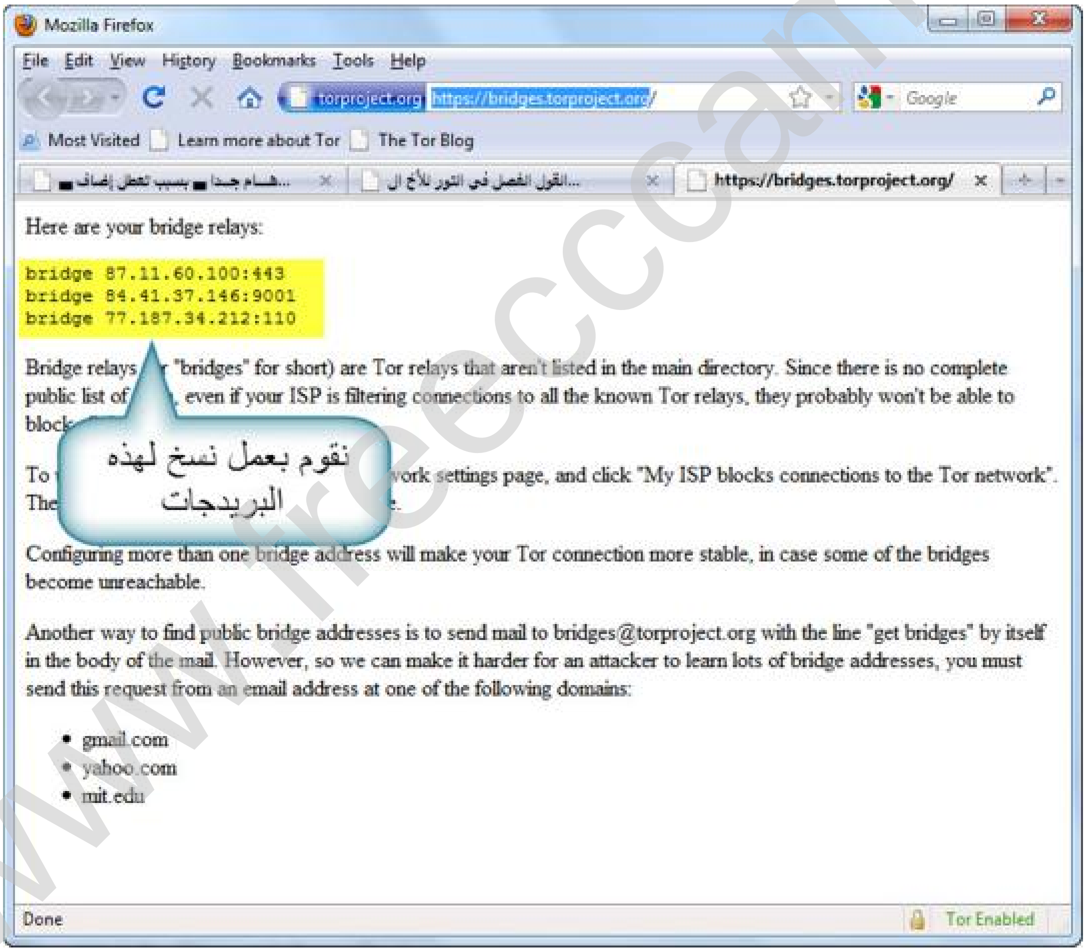
ملاحظة يمكنكم نقل البريدجات الثلاثة في نفس الوقت ومعها نصوص **Bridge**

هكذا مثلا فسيقبلها برنامج **ipnetinfo**

Bridge xx.xx.x.xx:xxxx

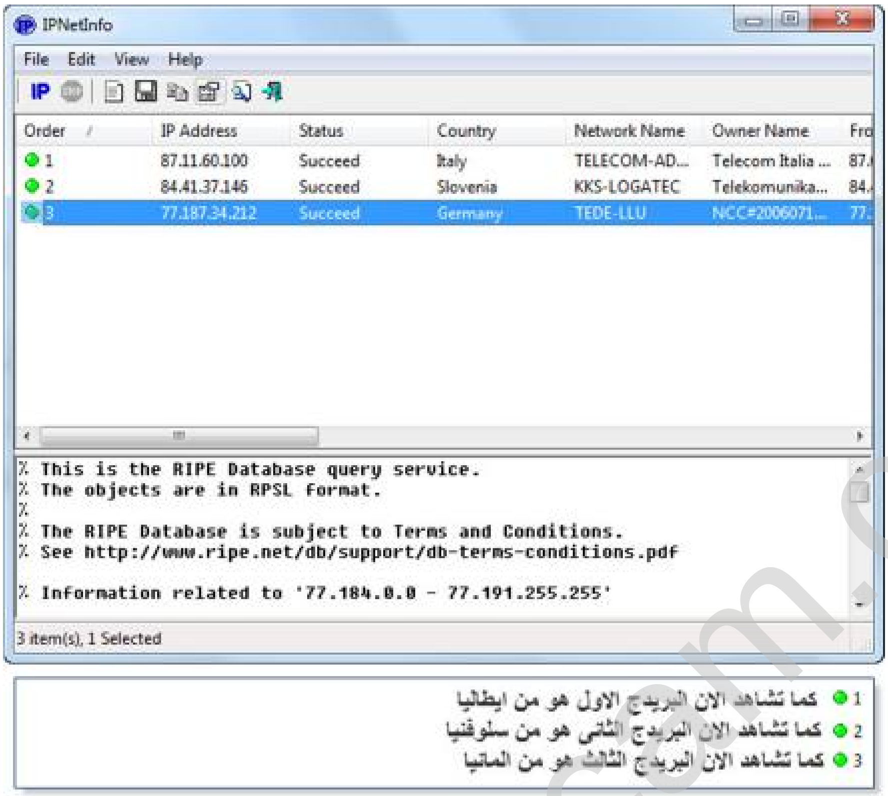
Bridge xx.xxx.xx.xx:xxx

Bridge xx.xx.xxx.xx:xx




Name
Date modified
Type
Size
ipnetinfo
5/5/2011 9:26 PM
Compiled HTML ...
ipnetinfo
5/5/2011 9:00 PM
Application
6/7/2011 6:32 PM
WinRAR ZIP archive
readme
5/5/2011 9:26 PM
Text Document
هذا هو البرنامج نقوم
بالضغط عليه دبل كليك
من اجل تشغليه


Choose IP Addresses
Type a single IP address or multiple IP addresses separated by commas, spaces, or CRLF. You can also paste the message headers from your email software, and the IP addresses will automatically be extracted from them.
bridge 87.11.60.100:443
bridge 84.41.37.146:9001
bridge 77.187.34.212:110
كما تشاهد الان هنا قم بلصق
البريدجات
Automatically use the right server according to IP address
Resolve IP addresses
Convert host names to IP addresses.
Load only the last IP address.
Pause for
30
Seconds
After retrieving
10
IP addresses
OK
Cancel
Clear
Paste



كما تشاهد الان ظهرت النتيجة في البرنامج وعرفنا مصدر البريدجات

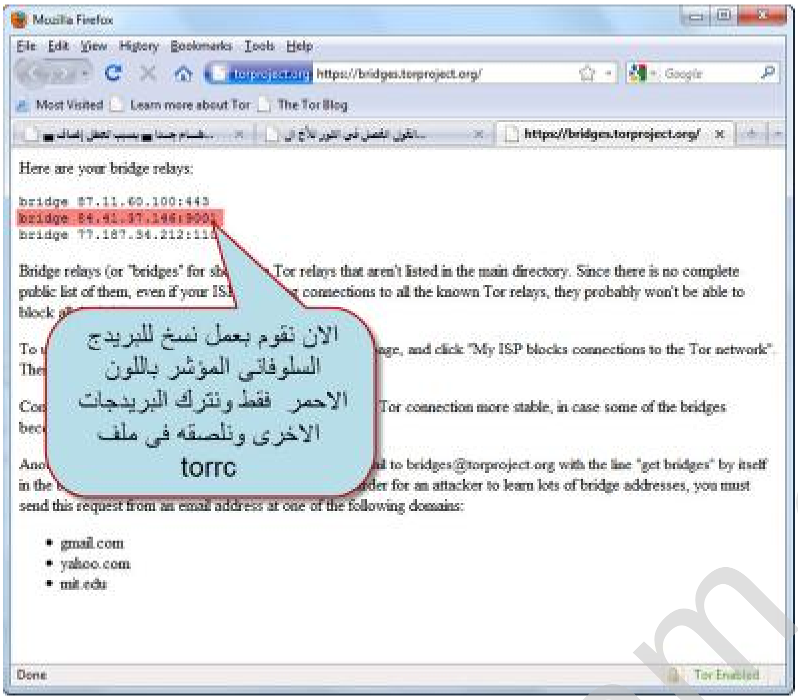
- **البريدج الاول** هو من ⬅ ايطاليا
- **البريدج الثانى** هو من ⬅ سلوفنيا
- **البريدج الثالث** هو من ⬅ المانيا

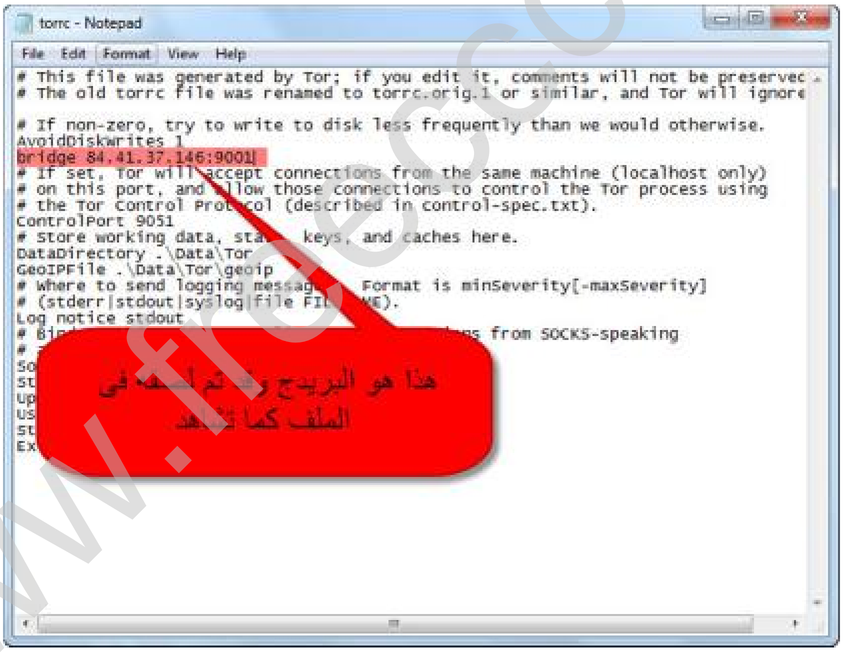
فـي هـذه الحالـة الان نقـوم باسـتبعاد البريـدج الإيطـالي والبريـدج الألمـاني واسـتعمال البريـدج السلوفانى كما تشاهد في الصور التالية

OK بعد الحصول على عدد لا بأس به من البريدجات نقوم بلصق هذه البريدجات الموثوقة في ملف **torrc** الموجود على هذا المسار (**Tor Browser/Data/Tor/torrc**) (يتم فتح ملف torrc بواسطة برنامج المفكرة notepad) كما تشاهد في الصور التالية

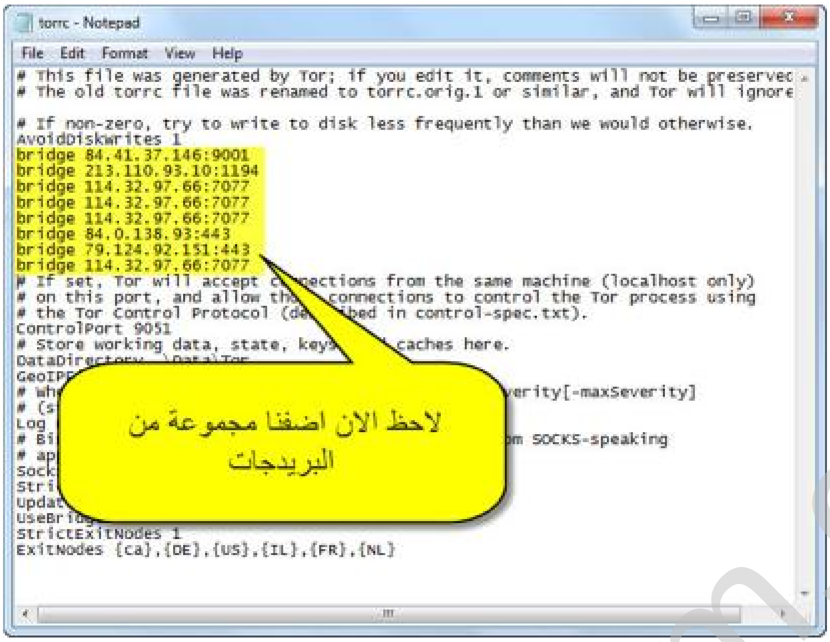
و اذا كنت تستعمل التور المثبت الملف يكون على هذا المسار

start/all programs/vidalia/tor





ثم نقوم بتكرار عملية البحث عن بريدجات جديدة حتى يصبح لدينا مجموعة كبيرة من البريدجات الغير تابعة لأى دولة من الدول المعادية لنا



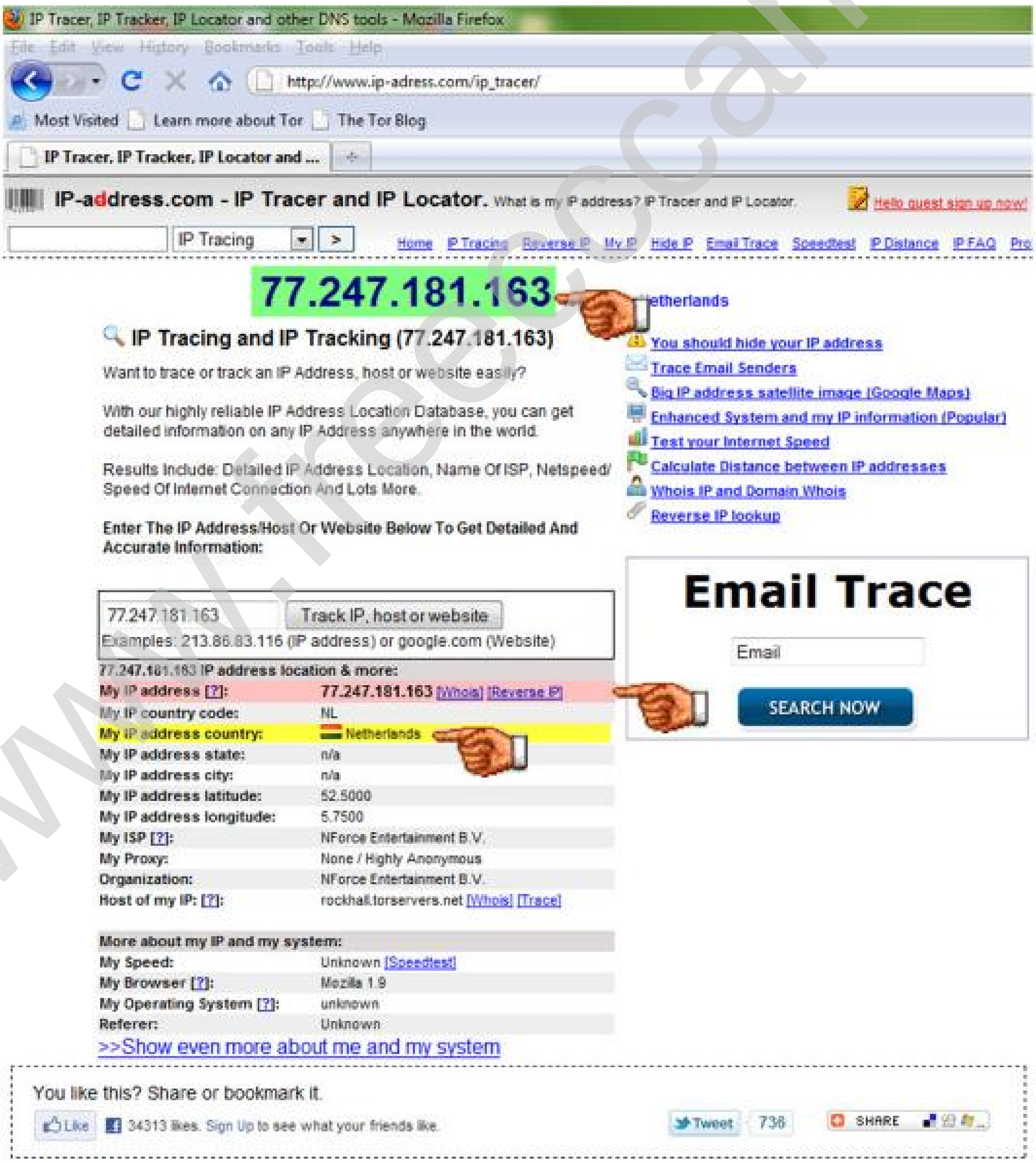
ملاحظة مهمة جدا

من اجل الحصول على مجموعة من البريدجات من الموقع عليك القيام بتغير هويتك بهذه الطريقة من اجل الحصول على بريدجات جديدة ثم قم بتحديث الصفحة الرئيسية للموقع



يمكنك الدخول الى هذا الموقع بعد تشغيل برنامج تور لمعرفة بلد الايبى الخاص بك الذى حصلت عليه عند اختيار هوية جديدة كما تشاهد في الصورة التالية
اصبح الايبى الخاص من هولندا
وكلما قمت بطلب وعمل هواية جديدة سوف تحصل على ايبى مختلف ودولة مختلفة

http://www. www.ip-adress.com/ip_tracer http://www.ip-adress.com	Web
في حالة عدم عمل رابط عنوان الموقع في الموضوع تم ارفاق ملف تكست يحتوى على رابط الموقع – اسم الملف **IP-ADRESS**	



هنا مثال من ملف **TORCC** تجدون في الاسفل مثال كامل يمكنكم الاقتداء به

This file was generated by Tor; if you edit it, comments will not be #
preserved
The old torrc file was renamed to torrc.orig.1 or similar, and Tor will #
ignore it

If non-zero, try to write to disk less frequently than we would #
.otherwise
AvoidDiskWrites 1
Bridge xx.xx.xxx.xx:xx
Bridge xx.xx.xxx.xx:xx
Bridge xx.xx.xxx.xx:xx
Bridge xx.xx.xxx.xx:xx
Bridge xx.xx.xxx.xx:xx
Bridge xx.xx.xxx.xx:xx
Bridge xx.xx.xxx.xx:xx
Bridge xx.xx.xxx.xx:xx
If set, Tor will accept connections from the same machine (localhost #
(only
on this port, and allow those connections to control the Tor process #
using
.(the Tor Control Protocol (described in control-spec.txt #
ControlPort 9051
.Store working data, state, keys, and caches here #
DataDirectory .\Data\Tor
A list of preferred nodes to use for the last hop in circuits, when #
.possible #
GeoIPFile .\Data\Tor\geoip
HashedControlPassword xx.xx.xxx.xx:xx
[Where to send logging messages. Format is minSeverity[-maxSeverity #
.(stderr|stdout|syslog|file FILENAME) #
Log notice stdout
Bind to this address to listen to connections from SOCKS-speaking #
.applications #
SocksListenAddress 127.0.0.1
If set, Tor will fail to operate when none of the configured ExitNodes #
can
.be used #
StrictExitNodes 1
UpdateBridgesFromAuthority 0
0**UseBridges**

StrictExitNodes 1
{ExitNodes {ca

في اول الكود وضعت قائمة البريدجات ستجدون قائمة قد وضعها التور ابدلوها بالقائمة الجديدة

النصوص الملونة باللون الاحمر في اخر الملف هامة جدا

قلنا ان العقدة الاخيرة تزيل آخر تشفير اذن تحصل على المعلومة غير مشفرة وسترسلها الى الموقع المتوجه اليه مثلا الفيس بوك.
هنا معلومات خطيرتان تقعا في يد آخر عقدة !وهما: المعلومة المرسلة والوجهة موقع الفيس بوك
وكما تعلمون فان العقد هي ايضا مثل البريدجات اي ان مستعملون يقومون بوضعها ! اذن من الممكن ان تكون عقدة الخروج لجهة امنية.

لاطلاع على عقد الخروج اضغط على زر **view the network** في واجهة التور فستحصلون على الخارطة ومعها قائمة العقد ويمكنكم ترتيبها حسب الدولة مثلا كما تشاهد في الصور التالية





هذه ستعطيكم فكرة عن العقد الموجوده (الى اي دولة تنتمي , ما مدى "صحتها" اذا كانت بصحة سيئة تكون هنالك درجة واحدة باللون البرتقالي
ان كانت ميته تكون سوداء
وان كانت جيدة تجد ثلاث درجات

سنزيل قائمة عقد الخروج في امريكا ومن لف لفها !

- هنا ابقيت فقط على عقد الخروج في كندا

كود:

```
StrictExitNodes 1ExitNodes {ca}
```

كان هذا للمثال فقط بامكانكم مثلا ابقاء الجميع وازالة فقط من تريدون.

- هنا مثلا حذفت كل المخارج التي توجد في المانيا وامريكاوالكيان الصهيوني هكذا

كود:

```
StrictExitNodes 0ExcludeExitNodes {de},{us},{IL}
```

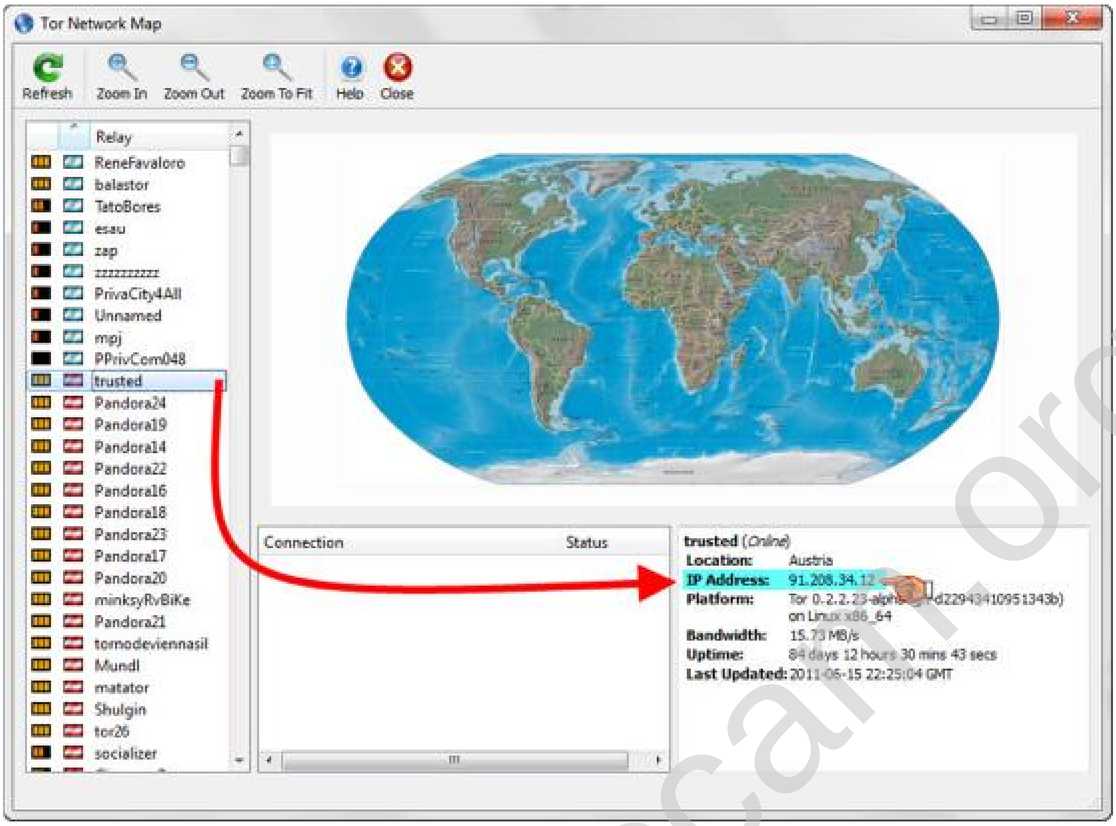
يجب ان لايكون هنالك مسافة بين الفواصل .

بإمكانكم بدل حذف دول كاملة ان تحذف فقط عُقد معينة بإدخال الآيبي خاصتها :

كود:

```
StrictExitNodes 0ExcludeExitNodes 192.251.226.206,76.73.41.180
```

- تأخذون الآيبي من هنا شاهد الصورة التالية:


Tor Network Map
Refresh
Zoom In
Zoom Out
Zoom To Fit
Help
Close
Relay
ReneFavaloro
balastor
TatoBores
esau
zap
zzzzzzzzzz
PrivaCity4All
Unnamed
mpj
PPrivCom048
trusted
Pandora24
Pandora19
Pandora14
Pandora22
Pandora16
Pandora18
Pandora23
Pandora17
Pandora20
minksyRvBiKe
Pandora21
tornodeviennasil
Mundl
matator
Shulgin
tor26
socializer
Connection
Status
trusted (Online)
Location: Austria
IP Address: 91.208.34.12
on Linux x86_64
Bandwidth: 15.73 MB/s
Uptime: 84 days 12 hours 30 mins 43 secs
Last Updated: 2011-05-15 22:25:04 GMT

المرحلة الثانية

تحدثنا سابقا عن "فلترة" البريدجات (مداخل شبكة التور) و تحدثنا عن اختيار مخارج معينة (حسب البلد مثلا او بإزالة بعض العقد فقط).

○ الآن سنقوم بإزالة بعض العقد في داخل الشبكة لماذا ذلك ونحن نعلم ان اخطر نقاط التور ليست في داخله بل في اطرافه ؟؟

☑ في الحقيقة هنالك عدة أسباب تجعلنا نُجهز على بعض العقد داخل الشبكة من تلك الأسباب: ان بعض العقد هي نقاط تفتيش ! وهي مشبوهة مخابراتية و لم توضع عبثا. و الوقاية احسن من العلاج (ان شاء الله ايضا سنعود لنتحدث عن الخطر الممكن).

☑ تلك العقد تعالج المعلومات اي تحاول فلترتها وتمحيصها فهي تقوم بتعطيل سرعة الاتصال بشكل كبير لذلك إزالتها ستساهم في رفع سرعة الاتصال !

ملاحظة مهمة : عند تطبيق هذه الطريقة لا تلمسوا ابدا settings في واجهة التور.

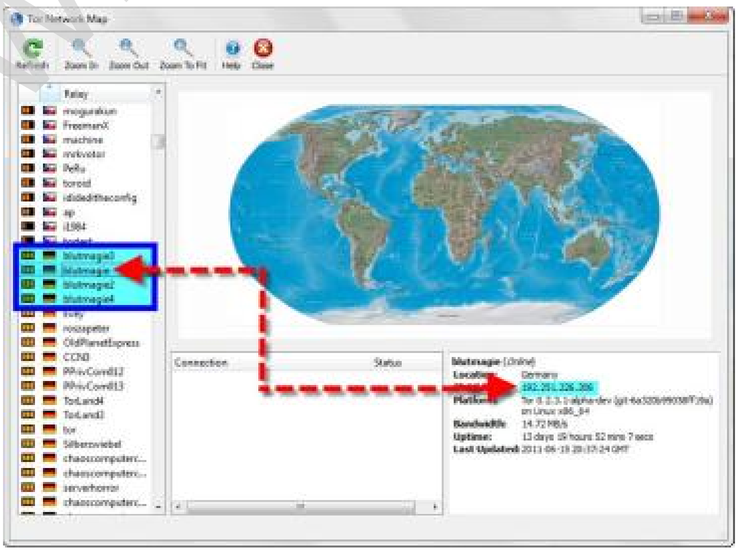


طريقة الكشف و الإزالة

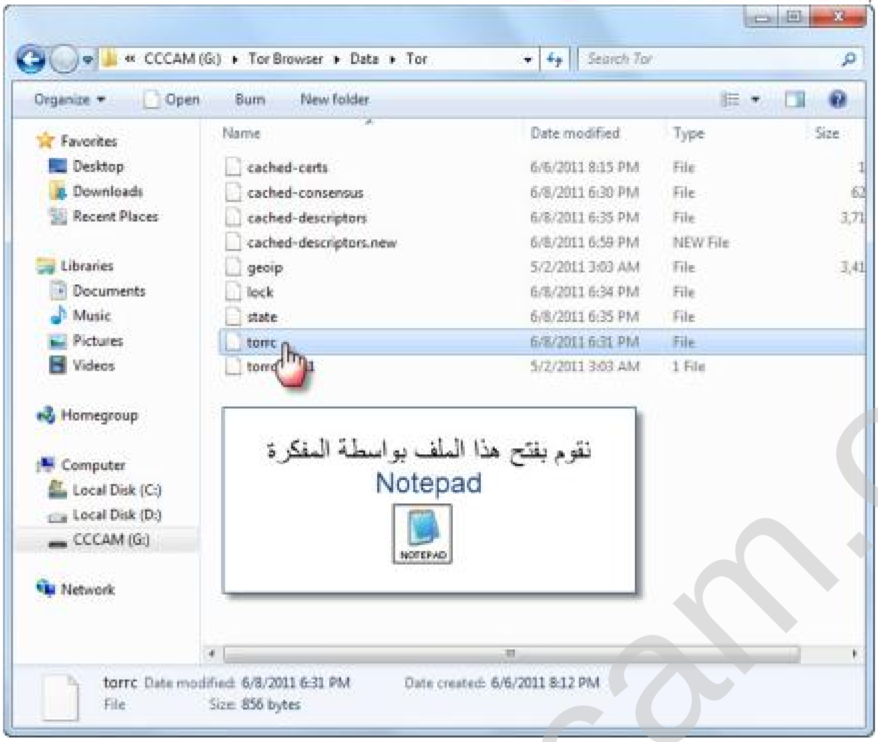
نقوم بفتح خارطة العقد بالضغط على زر view the network

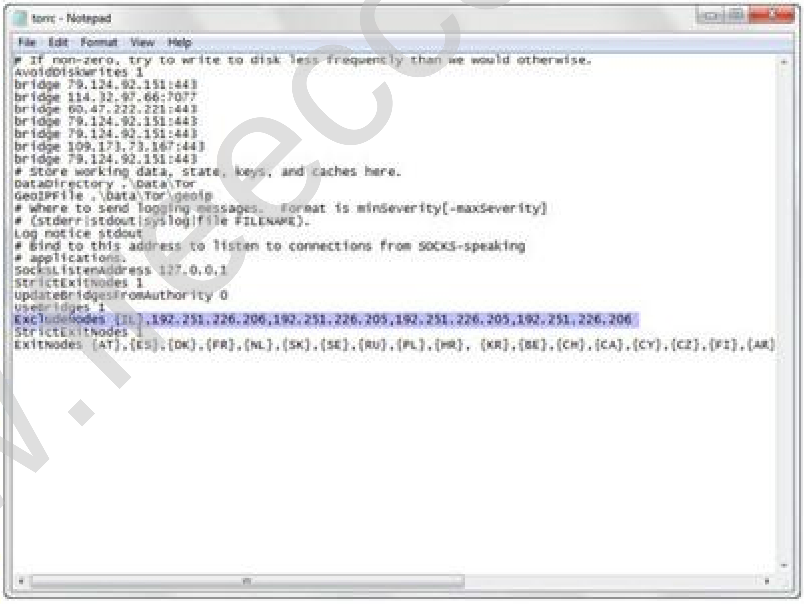
☑ تحصلون على الخارطة, ترتبون العقد حسب الدولة بالضغط على الزر المحاط بالأزرق.

نلاحظ هنا ان هنالك عقد دائمة التواجد مثل العقد التي اسمها **blutmagie** و المتواجدة في الدولة ذات السمعة السيئة المانيا انظر للصور

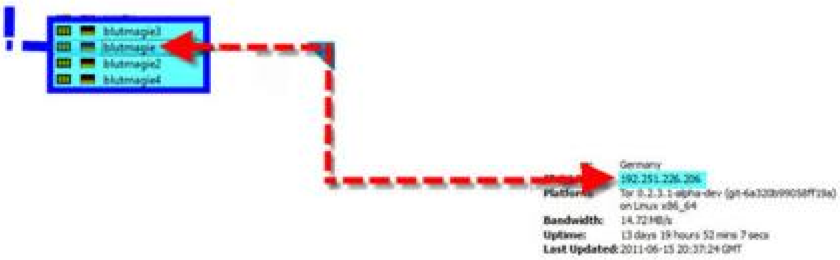


سنقوم بإزالتها من طريقنا الى الابد هكذا.





السطر الذي بالأزرق لوناه هو الذي قمنا من خلاله بإزالة عقد **blutmagie** وكذلك الكيان الصهيوني وبذلك المعلومات لن تمر ابدا بها.

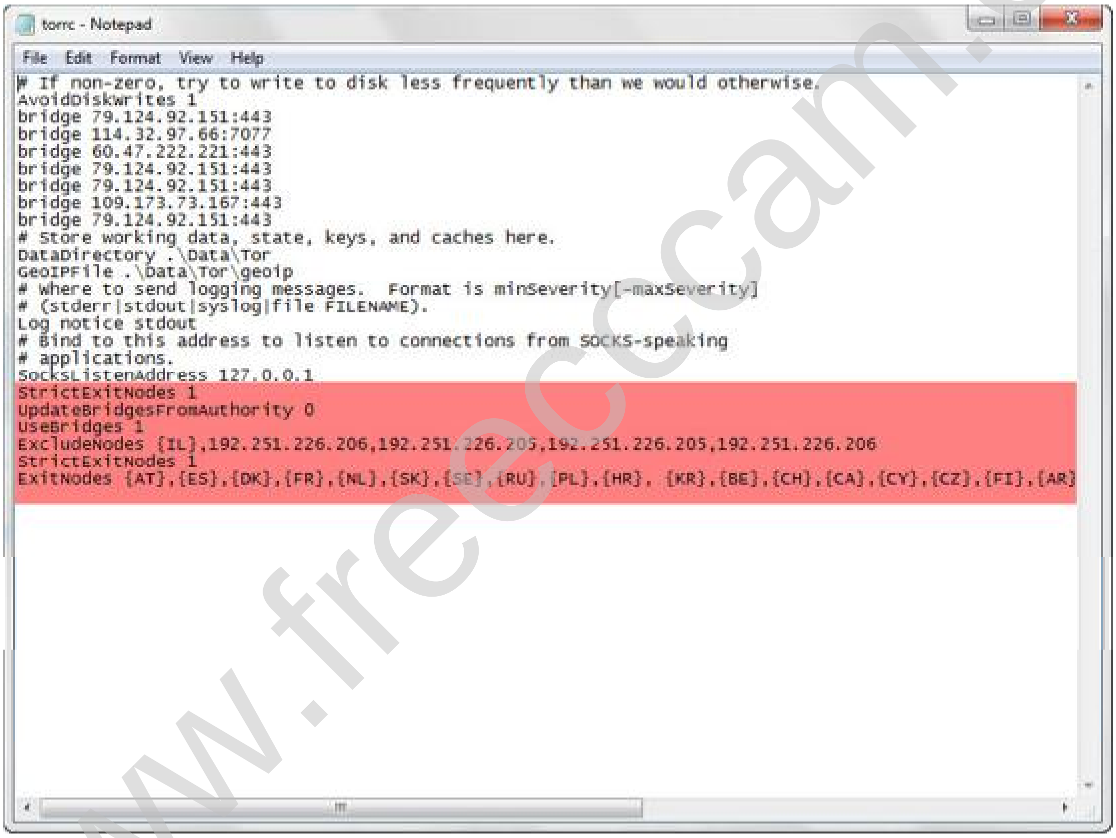




بعد هذا قوموا بإغلاق شبكة التور من هنا دون غلق واجهة البرنامج
واعادة تشغيل البرنامج بالضغط مرة اخرى على نفس الزر
ستلاحظون ان سرعة الشبكة قد تحسنت هذا ما لاحظته طبعا يمكنكم من بعد العثور على بعض العقد "الخبيثة" ذات الأسماء المريبة ! وحذفها
كما قلنا سابقا يمكنك اضافة هذا الكود في اسفل ملف) Tor Browser/Data/Tor/torrc
(يتم فتح ملف torrc بواسطة برنامج المفكرة notepad) كما تشاهد في الصور التالية

و اذا كنت تستعمل التور المثبت الملف يكون على هذا المسار

start/all programs/vidalia/tor


```
torrc - Notepad
File  Edit  Format  View  Help
# If non-zero, try to write to disk less frequently than we would otherwise.
AvoidDiskWrites 1
bridge 79.124.92.151:443
bridge 114.32.97.66:7077
bridge 60.47.222.221:443
bridge 79.124.92.151:443
bridge 79.124.92.151:443
bridge 109.173.73.167:443
bridge 79.124.92.151:443
# Store working data, state, keys, and caches here.
DataDirectory .\Data\Tor
GeoIPFile .\Data\Tor\geoip
# Where to send logging messages.  Format is minSeverity[-maxSeverity]
# (stderr|stdout|syslog|file FILENAME).
Log notice stdout
# Bind to this address to listen to connections from SOCKS-speaking
# applications.
SocksListenAddress 127.0.0.1
StrictExitNodes 1
UpdateBridgesFromAuthority 0
UseBridges 1
ExcludeNodes {IL},192.251.226.206,192.251.226.205,192.251.226.205,192.251.226.206
StrictExitNodes 1
ExitNodes {AT},{ES},{DK},{FR},{NL},{SK},{SE},{RU},{PL},{HR}, {KR},{BE},{CH},{CA},{CY},{CZ},{FI},{AR}
```

يمكنك تحميل الكود

http://www.freecccam.org/wordpress/wp-pic/Cood-001.zip	
في حالة عدم عمل رابط تحميل الملف في الموضوع تم ارفاق ملف الكود – اسم الملف **COOD-001**	

انا حددت الدول التي يمكن ان تكون مخارج لشبكة التور**(EXCLUDEEXITNODES)** تقوم بتسهيل المهمة لأنها تستثني بعض الدول من المخارج وتبقي الجميع لكنها ليست ثابتة فلا نستعملها حتى اصدار جديد ثابت.

بإمكانكم استعمال خارطة التور **(VIES THE NETWORK)** لإضافة الدول التي تأوي مخارج لشبكة التور. طبعا نستثني من ذلك الصهاينة والامريكان وربيبتهم المانيا وربما



بعض الدول التي يوجد فيها مخرجا او اثنين فقط ربحا للوقت

في هذا الموقع تجدون جميع كودات بلدان العالم

http://www.iso.org/iso/eng/country_codes/iso_3166_code_lists/english_country_names_and_code_elements.htm#i..
في حالة عدم عمل رابط الموقع في الموضوع تم ارفاق ملف تكست به رابط الموقع – اسم الملف **ISO-CODE**

خلاصة الموضوع

مراحل العمل:

A اختيار بريدجات معينة لدخول شبكة التور لان البريدجات مصدر خطر كبير (هي تحوي على "صيد" ثمين باحتوائها على آيبي خاصتنا و المسلك الذي ستمر به وجهتها الاخيرة وهي معلومات مشفرة....لكن ملة الكفر واحدة !)

B اختيار مخارج "آمنة "من الشبكة لأن المخارج تكون المعلومة فيها مكشوفة وغير مشفرة: محتوى المعلومة مكشفة ووجهتا (موقع جهادي)كذلك لكن مصدرها غير معلوم.

C ازالت عقد داخل الشبكة. هي عبارة عن نقاط تفتيش للتجسس تقوم بالفلترة والتمحيص اي تخفيض سرعة تبادل المعلومات وبالتالي تعطيل التصفح.

النتائج:

التأمين وزيادة سرعة الشبكة وبالتالي التصفح

اضافة مهمة للعمل مع تور

HTTPS EveryWhere



ينصح موقع التور بإضافة للفايرفوكس اسمها Https AnyWhere وظيفتها تشفير المعلومات والبيانات أثناء طلبنا للمواقع فمثلا عند طلبنا موقع الفيس بوك عن طريق الرابط المشفر فإن آخر عقدة من التور سترسل المعلومات لموقع الفيس بوك تكون مشفرة ويقوم موقع الفيس بوك بفك التشفير

أما عند عدم استخدامنا لخاصية الرابط المشفر في موقع الفيس بوك فإن العقدة الأخيرة في التور ستفك آخر تشفير للمعلومة التي ارسلناها وستعلم محتوى المعلومة وتقوم بإرسالها غير مشفرة



طيب ماذا عن المواقع الأخرى مثل Google.com فعندما نقوم بالبحث من خلال موقع غوغل الغير مشفر فإن العقدة الأخيرة للتور ستعلم محتوى المعلومة وسترسلها بشكل غير مشفر لغوغل أما عند طلبنا للرابط المشفر لموقع غوغل https://encrypted.google.com فإن آخر عقدة من التور سترسل المعلومة مشفرة لغوغل وسيقوم غوغل بفك تشفيرها

وهنا أمر هام فكلنا نبحث عن المواد الجهادية عن طريق موقع غوغل وقليل منا من يستخدم الرابط المشفر لغوغل وذلك امر خطير لا يجب الاستهانة به أبدا

فنحن كما نعلم أن من يضع آخر عقدة من عقد التور هم أيضا مستخدمون وقد تكون آخر من عقد التور التي نستخدمها حاليا مخابراتية

لنقوم باستثناء بعض العقد المشبوهة من عقدة الخروج ولكن ذلك لا يكفي فإن آخر عقدة ستفك آخر تشفير للمعلومة التي سنقوم بإرسالها فهي تعلم ((آخر عقدة)) محتوى المعلومة وتعلم وجهتها ولكنها لا تعلم الآيبي الخاص بنا

ولذلك ولكي يتم التغلب على مشكلة ان آخر عقدة من التور تعلم محتوى المعلومة فنقوم باستخدام الرابط المشفر للموقع حتى تقوم آخر عقدة من التور بإرسال المعلومة مشفرة ويقوم الموقع المراد بفك تشفير المعلومة ..

وكذلك لا ننسى أن الثوار الاحرار العاملين يهمهم تشفير المعلومة التي يرسلونها بشكل كامل وبالأخص لموقعي الشبكات الاجتماعية لنشر تطور الاحداث



FACEBOOK.COM و **YOUTUBE.COM** و موقع **TWITTER** فإضافة **HTTPS EveryWhere** تقوم بتحويل الرابط من **HTTP** إلى شكله المشفر **HTTS** اي فقط كل ماعلينا بعد تثبيت الإضافة أن نطلب موقع غوغل بشكله العادي الغير مشفر **GOOGLE.COM** وسنلاحظ أن إضافة **HTTPS EveryWhere** ستقوم بنقلنا إلى

الرابط المشفر لموقع غوغل **https**://encrypted.google.com والحال نفسه عند طلب موقع **FACEBOOK.COM** و **TWITTER.COM** والعديد من المواقع الهامة الأخرى التي نستخدمها



تابع الشرح المصور

اولا عليك التوجه الى الموقع الرسمي للإضافة من اجل تثبيت الاضافة مع متصفح الفايرفوكس

برنامج	https://www.eff.org/https-everywhere
	في حالة عدم عمل الرابط في الموضوع تم ارفاق ملف تكست يحتوى على رابط الموقع الرسمي لتحميل الاضافة – اسم الملف **HTTPS**



ELECTRONIC FRONTIER FOUNDATION

HOME | ABOUT | OUR WORK | DEEPLINKS BLOG | PRESS ROOM | TAKE ACTION | SHOP

Home » Our Work » EFF Software

HTTPS Everywhere

DONATE to EFF

JOIN EFF

Quick link: you can install the latest version of HTTPS Everywhere by clicking here.

HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

Many sites on the web offer some limited support for encryption over HTTPS, but make it difficult to use. For instance, they may default to unencrypted HTTP, or fill encrypted pages with links that go back to the unencrypted site.

The HTTPS Everywhere extension fixes these problems by rewriting all requests to these sites to HTTPS. Firefox users can get it by clicking here:

ENCRYPT THE WEB: INSTALL HTTPS EVERYWHERE

The plugin currently works for:

- Google Search
- Wikipedia
- Twitter
- Facebook
- bit.ly
- GMX
- Wordpress.com blogs
- The New York Times
- Paypal
- EFF
- Tor
- Ixquick
- and many other sites!

Sadly, many sites still include a lot of content from third party domains that is not available over HTTPS. As always, if the browser's lock icon is broken or carries an exclamation mark, you may remain vulnerable to some adversaries that use active attacks or traffic analysis. However, the effort that would be required to eavesdrop on your browsing should still be usefully increased.

Answers to common questions may be on the frequently asked questions page.

HTTPS Everywhere can protect you only when you're using sites that support HTTPS and for which HTTPS Everywhere includes rules. If sites you use don't support HTTPS, ask the site operators to add it; only the site operator is able to enable HTTPS. There is more information and instruction on how server operators can do that in the EFF article How to Deploy HTTPS Correctly.

Development And Writing your own Rulesets

You can help us test forthcoming site support and new features by installing the development branch of the extension.

HTTPS Everywhere uses small ruleset files to define which domains are redirected to https, and how. If you'd like to write your own ruleset, you can find out how to do that here.

Information about how to access the project's Git repository and get involved in development is here.

Send feedback on this project to the https-everywhere AT eff.org mailing list. Note that this is a public and publicly-archived mailing list. You can also subscribe.

Send new rewrite rules or fixes to existing rewrite rules to the https-everywhere-rules AT eff.org mailing list. Note that this is a public and publicly-archived mailing list. You can also subscribe.

Related Projects

Our code is partially based on the STS implementation from the groundbreaking NoScript project (there are other STS implementations out there, too).

HTTPS Everywhere aims to have a simpler user experience than NoScript, and to support complex rewriting rules that allow services like Google Search and Wikipedia to be redirected to HTTPS without breaking anything. It also handles situations like https:// pages that redirect back to http:// in a reasonable manner.

In an ideal world, every web request could be defaulted to HTTPS. Unfortunately, there's no way to know that what you get from requesting https://www.domain.com/page is the same as what you get from requesting http://www.domain.com/page. So the only way to switch every page to https is to fetch the page insecurely first. There is a Chrome extension called KB SSL Enforcer which attempts to take that approach, but it does not appear to be implemented securely: when we tested it, it seemed to always use http before https, which means that your surfing habits and authentication cookies are not protected (this may be a limitation of the Chrome Extensions framework).

License

HTTPS Everywhere is licensed under the GNU General Public License, version 2 or later. To get the source code, see the development page.

Attachment

https-everywhere-0.9.6.xpi
https-everywhere-0.9.9.develop...
https-everywhere-0.9.9.development.6...
Changelog.txt
https-everywhere-0.9.7.xpi 57.8 KB

Related Issues: Privacy



HTTPS Everywhere is licensed under the GNU General Public License, version 2 or later. To get the source code, see the development page.

Attachment

https-everywhere-0.9.6.xpi
https-everywhere-0.9.9.develop...
https-everywhere-0.9.9.development.6...
Changelog.txt
https-everywhere-0.9.7.xpi 57.8 KB

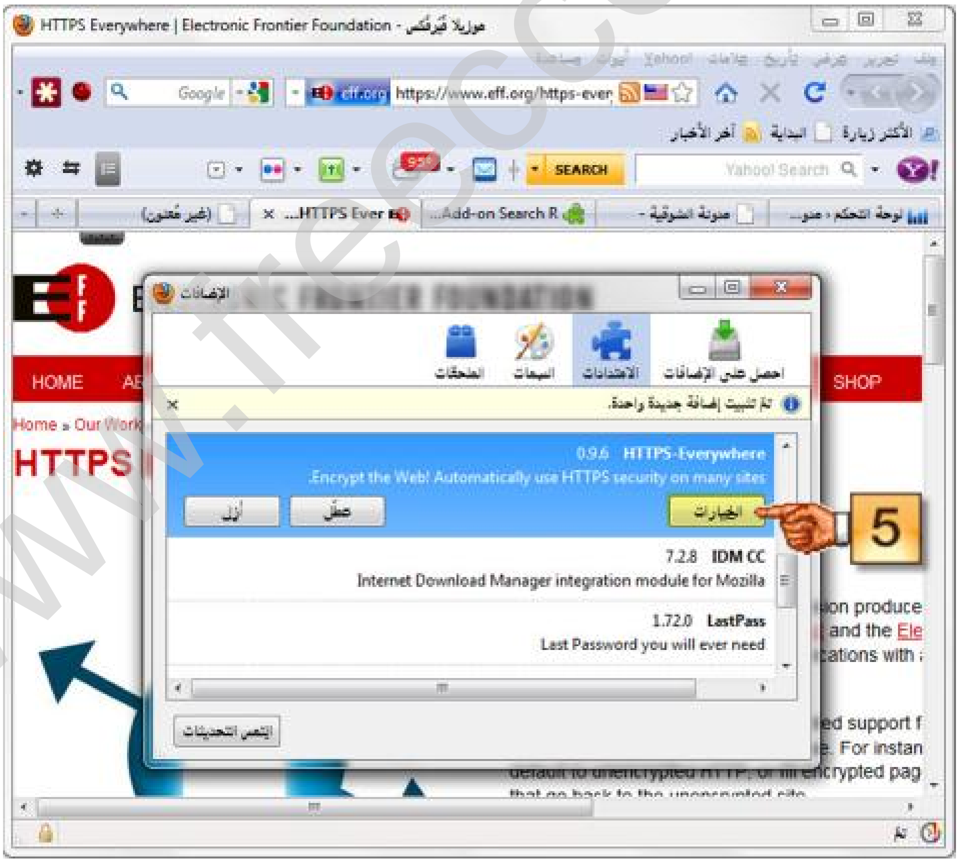
Related Issues: Privacy


موزيلا فَيَرفُكس
https://www.eff.org/files/https-every
فَيَرفُكس منع هذا الموقع (www.eff.org) من سؤالك تثبيت برنامج على جهازك.
اسمح
2


موزيلا فَيَرفُكس
https://www.eff.org/files/https-every
تثبيت البرمجيات
ثبّت الإضافات الصادرة عن المؤلفين الذين تثق بهم فقط
يمكن للبرمجيات الخبيثة أن تضرّ بالحاسوب أو تنتهك خصوصيتك
طُلب منك تثبيت العنصر التالي:
https-everywhere-0.9.6.xpi
https://www.eff.org/files/https-everywhere-0.9.6.xpi
ألغِ
ثبّت (5)
3



موزيلا فَيَرفُكس
ملف تحرير عرض تأريخ علامات Yahoo! أدوات مساعدة
https://www.eff.org/files/https-every
الإضافات
حصل على الإضافات الامتدادات السمات الملحقات التثبيت
أعد تشغيل فَيَرفُكس لإتمام تغييراتك.
أعد تشغيل فَيَرفُكس
4
0.9.6 HTTPS-Everywhere
أعد التشغيل لإكمال التثبيت.
ألغ



HTTPS Everywhere | Electronic Frontier Foundation - موزيلا فَيَرفُكس
https://www.eff.org/https-ever
الإضافات
احصل على الإضافات الامتدادات السمات الملحقات
تم تثبيت إضافة جديدة واحدة.
0.9.6 HTTPS-Everywhere
Encrypt the Web! Automatically use HTTPS security on many sites.
الخيارات عطّل أزل
5
7.2.8 IDM CC
Internet Download Manager integration module for Mozilla
1.7.2.0 LastPass
Last Password you will ever need
التمس التحديثات
HOME
SHOP
HTTPS


HTTPS Everywhere | Electronic Frontier Foundation - موزيلا فَيَرفُكس
https://www.eff.org/https-everywhere
HTTPS Everywhere Preferences
Which HTTPS redirection rules should apply?
Reset to Defaults
Disable All
المواقع التى يمكن الدخول لها بواسطة التشفير


Google - موزيلا فَيَرفُكس
https://encrypted.google.com/
شاهد كيف اصبح رابط موقع جوجل
https://encrypted.google.com
Google beta
انتقل إلى عرض Google الكلاسيكي
بحث Google
ضربة حظ
مزيد من المعلومات عن البحث في Google باستخدام SSL